AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An apparatus for encrypting/decrypting a real-time input stream, comprising:

a processor configured to receive a data stream of bytes wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, convert the data stream into data blocks, provide the data blocks for encryption or decryption, receive encrypted or decrypted data blocks, convert the received encrypted or decrypted data blocks into bytes, and output the bytes, wherein the processor generates a start key signal when a new round key is needed for every round;

a key schedule unit configured to provide a round key for every round in accordance with the start key signal and an input key having a variable size to provide the round key for the encryption or decryption for each round, wherein the input key size is one of 128, 192, and 256 bits; and

a block round unit configured to receive converted data blocks from the ~~control unit~~ processor, receive the round key from the key schedule unit, encrypt or decrypt the received data blocks, and provide the encrypted or decrypted data blocks to the ~~control unit~~ processor,

wherein the key schedule unit selects a 128 bit round key to the block round unit for ~~the~~ each round using a key register having a capacity of {(size of an inputted block)*(size of one round)}, and the key schedule unit provides the round key to the block round unit for each round without storing expanded keys being generated by the key schedule unit.

2. (Previously Presented) The apparatus of claim 1, wherein the processor comprises:

an input buffer configured to store the data stream of bytes and convert the received data stream into the data blocks having a predetermined size so as to output the converted data blocks to the block round unit; and

an output buffer configured to receive the data blocks encrypted or decrypted in the block round unit and convert the received data blocks into bytes so as to output a converted data.

3. (Currently Amended) The apparatus of claim 2, wherein the block round unit completes all round calculation of data having been currently encrypted or decrypted before a next data block is inputted from the processor and then stores the corresponding result in the output buffer of the ~~control unit~~ processor.

4. (Cancelled)

5. (Currently Amended) The apparatus of claim 1, wherein the key schedule unit comprises:

a key expansion unit configured to expand the inputted key value into a size amounting to {block size*(count of rounds +1)}; and

a key selection unit configured to ~~expand~~ select the 128 bit key required for each round from the expanded key value so as to provide the selected key to the block round unit.

6-8. (Cancelled)

9. (Previously Presented) The apparatus of claim 1, wherein the processor generates a control signal to produce the selected 128 bit round key every round and then outputs the control signal to the key schedule unit.

10. (Currently Amended) An apparatus for encrypting/decrypting a real-time input data stream wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, comprising:

a processor configured to receive a data stream in first data format, convert the data stream and ~~outputting~~ output data in a second data format for encryption or decryption, wherein the processor generates a start key signal when a new round key is needed for every round;

a key schedule unit in communication with the processor and configured to provide a round key for every round in response to the start key signal and an input key having a variable size for the encryption or decryption for each round, wherein the input key size is one of 128, 192, and 256 bits; and

a block round unit in communication with the processor and the key schedule unit and configured to receive converted data in second data format from the ~~control unit~~ processor, receive the round key value from the key schedule unit for encryption or decryption of each round, and provide the encrypted or decrypted result to the ~~control unit~~ processor,

wherein the key schedule unit expands the input key into a size of {second data format size * (count of rounds +1)}, selects an N bit key required for each round from the expanded key value, and provides the selected N bit key to the block round unit for each round, and the key schedule unit selects a 128 bit round key to the block round unit for ~~the~~ each round using a key register having a capacity of {(size of an inputted block)*(size of one round)}, and the key schedule unit provides the round key to the block round unit for each round without storing expanded keys being generated by the key schedule unit.

11. (Previously Presented) The apparatus of claim 10, wherein the first data format is in bytes, and the second data format is a data block.

12. (Previously Presented) The apparatus of claim 10, wherein the processor comprises:

an input buffer configured to store the data stream of the first data format and convert the received data stream into the data of the second data format having a predetermined size; and

an output buffer configured to receive data in the second data format and convert the data into the first data format.

13. (Currently Amended) The apparatus of claim 12, wherein the block round unit substantially completes all data encryption or decryption processing before a next set of data is inputted from the processor and stores the corresponding result in the output buffer of the ~~control unit~~ processor.

14-17. (Cancelled)

18. (Previously Presented) The apparatus of claim 10, wherein the N bit key is equal to

the 128 bit round key.

19-20. (Cancelled)

21. (Previously Presented) The apparatus of claim 10, wherein the processor generates a control signal to produce the round key in every round.

22. (Currently Amended) A real-time encryption/decryption apparatus, comprising:

a processor configured to receive a data stream in first data format wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, convert the data stream and output data in a second data format for encryption or decryption, wherein the processor generates a start key signal when a new round key is needed for every round;

a key schedule unit in communication with the processor and configured to provide a round key in a predetermined period in response to the start key signal and an input key having a variable size, wherein the input key size is one of 128, 192, and 256 bits, and the key schedule unit has a key register capable of processing the input key required for the predetermined period; and

a block round unit in communication with the processor and the key schedule unit and configured to receive converted data in second data format from the ~~control unit~~ processor, and receive the round key from the key schedule unit for encryption or decryption of each round,

wherein a size of the key register is no less than {(second data format size)*(size of one period)}, and the key schedule unit provides the round key to the block round unit for each round without storing expanded keys being generated by the key schedule unit.

23. (Previously Presented) The apparatus of claim 22, wherein the first data format is in bytes, and the second data format is a data block.

24. (Cancelled)

25. (Currently Amended) A method of controlling a data protection key, the method

being processed in an encryption apparatus, comprising:

~~generating a start key signal using a processor when a generation of a new data key is needed for every round in the encryption apparatus;~~

generating a new data protection key according to ~~the~~ a start key signal, the start key signal generated when a generation of the new data protection key is needed in the encryption apparatus, the new data protection key generated according to ~~at least one of~~ a predetermined period ~~and a scheduled period in the encryption apparatus, wherein the scheduled period depends on a change of size of the new data key~~, wherein the new data protection key is generated through an intermediate value, and the intermediate value is not stored; and

encrypting data corresponding to the period with the new data protection key in the encryption apparatus.

26. (Previously Presented) The method of claim 25, further comprising a data key valid signal provided with the new data key for encryption or decryption.

27. (Previously Presented) The method of claim 25, wherein the data are encrypted according to the start key signal in real time.